
STATUTORY INSTRUMENTS

2022 No. 933

**The Electronic Communications
(Security Measures) Regulations 2022**

Supply chain

7.—(1) A network provider or service provider must take such measures as are appropriate and proportionate to identify and reduce the risks of security compromises occurring in relation to the public electronic communications network or public electronic communications service as a result of things done or omitted by third party suppliers.

(2) In this regulation, “third party supplier”, in relation to a network provider or service provider, means a person who supplies, provides or makes available goods, services or facilities for use in connection with the provision of the public electronic communications network or public electronic communications service.

(3) The risks referred to in paragraph (1) include—

- (a) those arising during the formation, existence or termination of contracts with third party suppliers, and
- (b) those arising from third party suppliers with whom the network provider or service provider has a contractual relationship contracting with other persons for the supply, provision or making available of any goods, services or facilities for use in connection with the provision of the public electronic communications network or public electronic communications service.

(4) A network provider or service provider (“the primary provider”) must take such measures as are appropriate and proportionate—

- (a) to ensure, by means of contractual arrangements, that each third party supplier—
 - (i) takes appropriate measures to identify the risks of security compromises occurring in relation to the primary provider’s network or service as a result of the primary provider’s use of goods, services or facilities supplied, provided or made available by the third party supplier, to disclose any such risks to the primary provider, and to reduce any such risks,
 - (ii) where the third party supplier is itself a network provider and is given access to the primary provider’s network or service or to sensitive data, takes appropriate measures for the purposes mentioned in section 105A(1) of the Act, in relation to goods, services or facilities supplied, provided or made available by the third party supplier to the primary provider, which are equivalent to the measures that the primary provider is required to take in relation to the primary provider’s network or service,
 - (iii) takes appropriate measures to enable the primary provider to monitor all activity undertaken or arranged by the third party supplier in relation to the primary provider’s network or service, and
 - (iv) takes appropriate measures to co-operate with the primary provider in the resolution of incidents which cause or contribute to the occurrence of a security compromise

in relation to the primary provider's network or service or of an increased risk of such a compromise occurring,

- (b) to ensure that all network connections and data sharing with third party suppliers, or arranged by third party suppliers, are managed securely, and
 - (c) to have appropriate written plans to manage the termination of, and transition from, contracts with third party suppliers while maintaining the security of the network or service.
- (5) A network provider must—
- (a) ensure that there is in place at all times a written plan to maintain the normal operation of the public electronic communications network in the event that the supply, provision or making available of goods, services or facilities by a third party supplier is interrupted, and
 - (b) review that plan on a regular basis.

Commencement Information

II [Reg. 7](#) in force at 1.10.2022, see [reg. 1\(2\)](#)

Changes to legislation:

There are currently no known outstanding effects for the The Electronic Communications (Security Measures) Regulations 2022, Section 7.